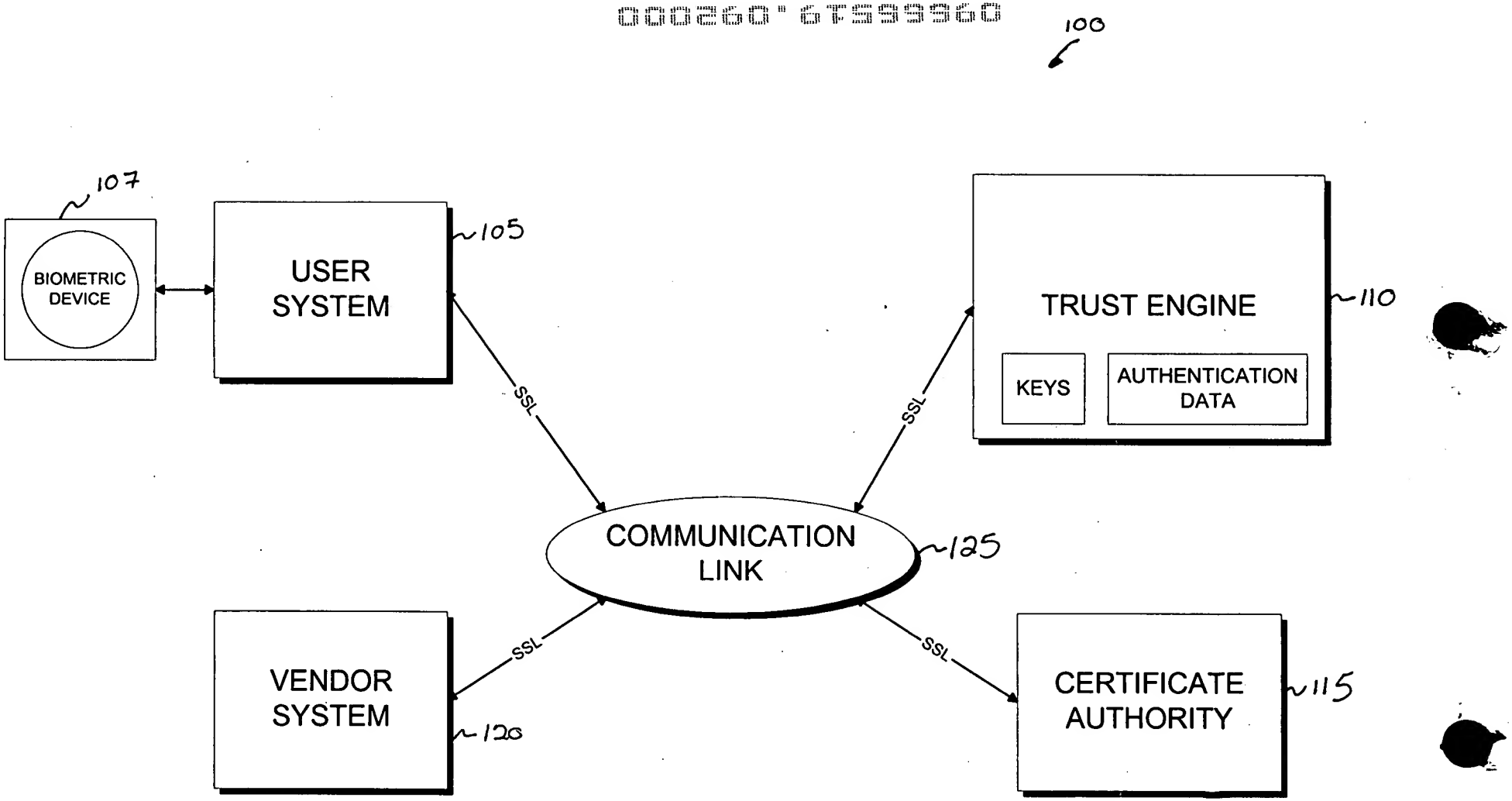


FIG. 1

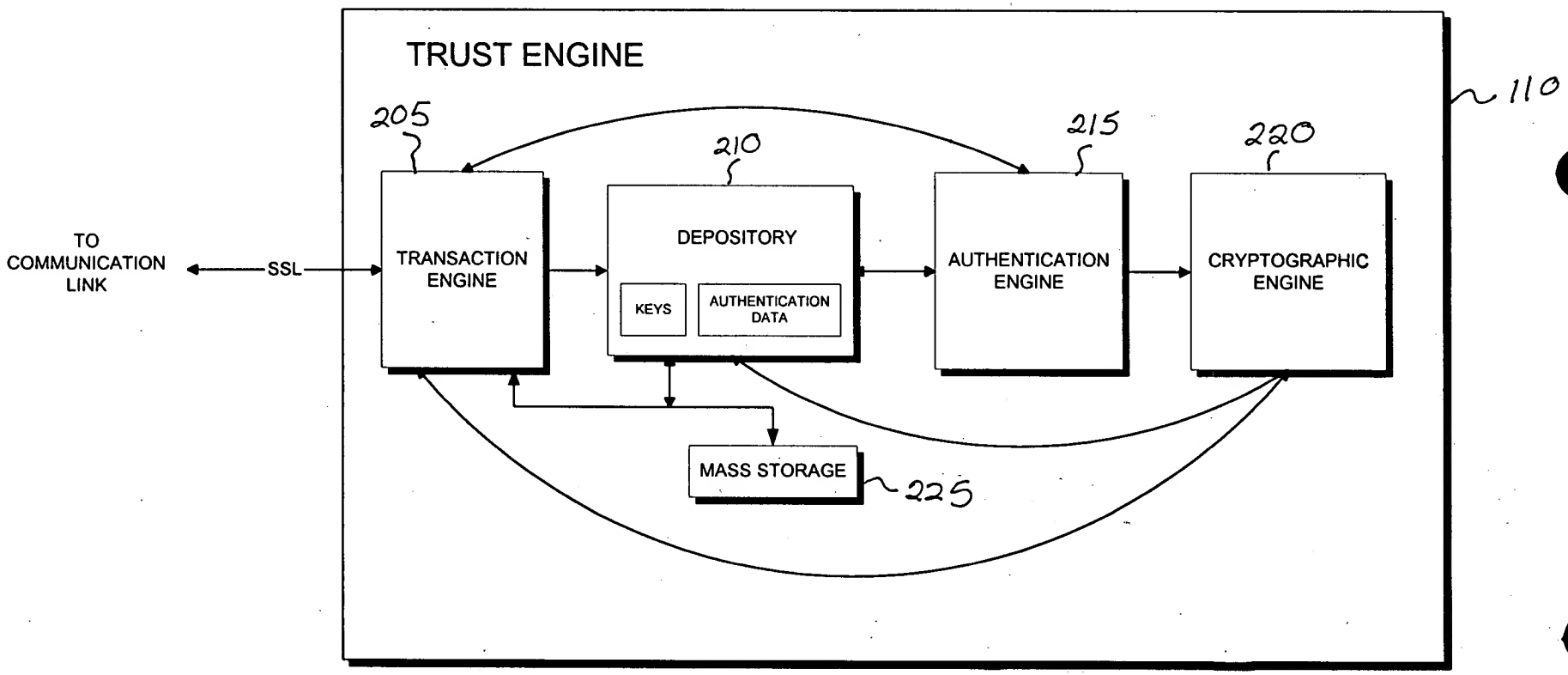

TRUST ENGINE
110
205
210
215
220
TO COMMUNICATION LINK
SSL
TRANSACTION ENGINE
DEPOSITORY
KEYS
AUTHENTICATION DATA
AUTHENTICATION ENGINE
CRYPTOGRAPHIC ENGINE
MASS STORAGE
225

FIG. 2

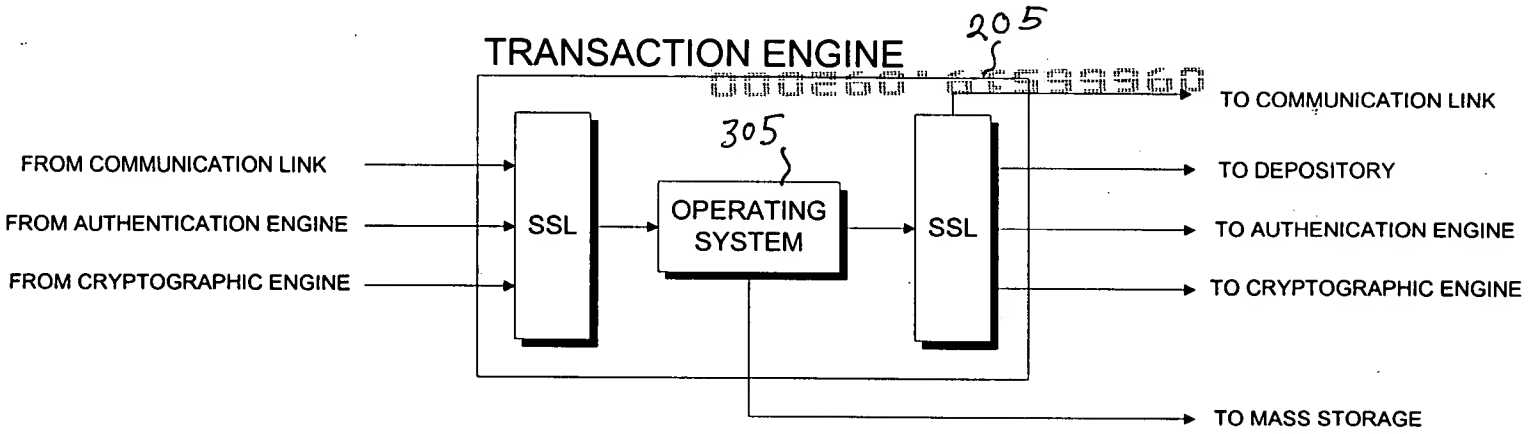

TRANSACTION ENGINE
205
305
FROM COMMUNICATION LINK
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
SSL
OPERATING SYSTEM
SSL
TO COMMUNICATION LINK
TO DEPOSITORY
TO AUTHENICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
TO MASS STORAGE

FIG. 3

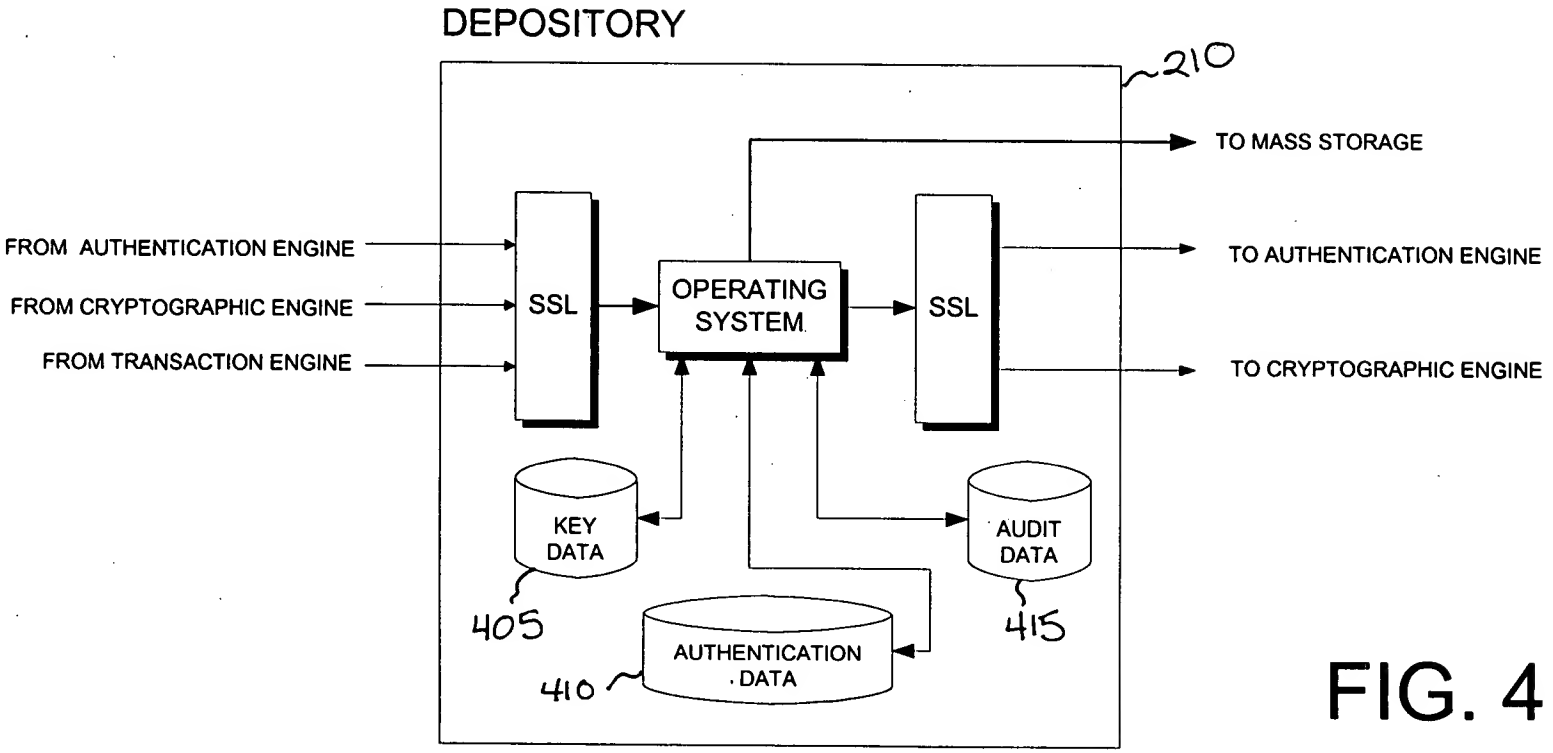

DEPOSITORY
210
FROM AUTHENTICATION ENGINE
FROM CRYPTOGRAPHIC ENGINE
FROM TRANSACTION ENGINE
SSL
OPERATING SYSTEM
SSL
TO MASS STORAGE
TO AUTHENTICATION ENGINE
TO CRYPTOGRAPHIC ENGINE
KEY DATA
AUDIT DATA
405
415
AUTHENTICATION DATA
410

FIG. 4

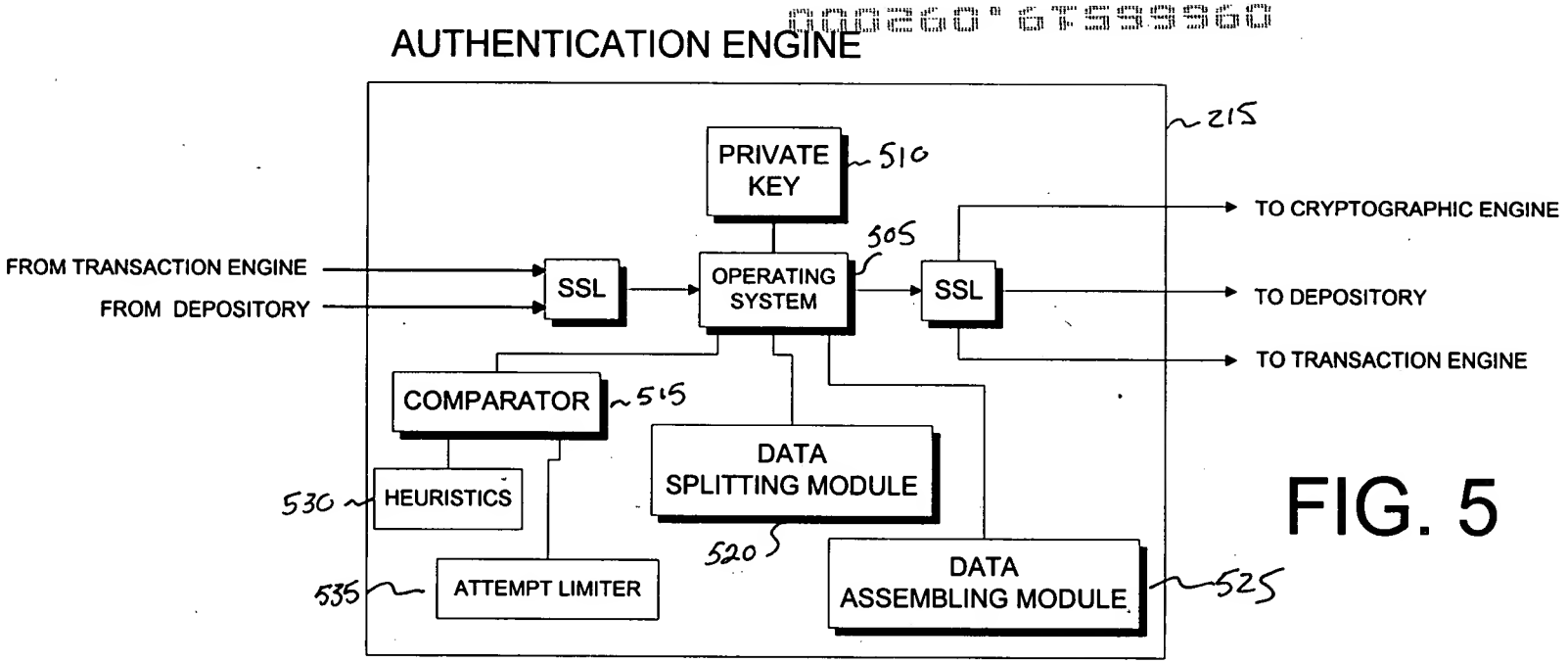

AUTHENTICATION ENGINE
215
PRIVATE KEY
510
505
FROM TRANSACTION ENGINE
FROM DEPOSITORY
SSL
OPERATING SYSTEM
SSL
TO CRYPTOGRAPHIC ENGINE
TO DEPOSITORY
TO TRANSACTION ENGINE
COMPARATOR
515
DATA SPLITTING MODULE
530
HEURISTICS
520
535
ATTEMPT LIMITER
DATA ASSEMBLING MODULE
525

FIG. 5

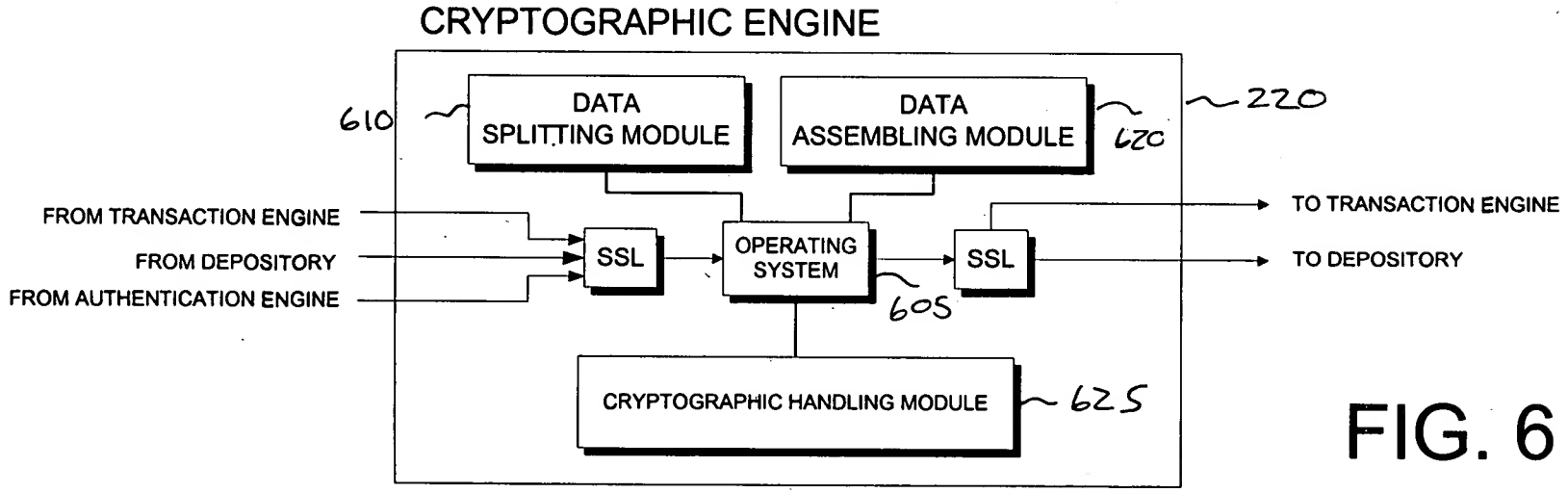

CRYPTOGRAPHIC ENGINE
610
DATA SPLITTING MODULE
DATA ASSEMBLING MODULE
620
220
FROM TRANSACTION ENGINE
FROM DEPOSITORY
FROM AUTHENTICATION ENGINE
SSL
OPERATING SYSTEM
SSL
605
TO TRANSACTION ENGINE
TO DEPOSITORY
CRYPTOGRAPHIC HANDLING MODULE
625

FIG. 6

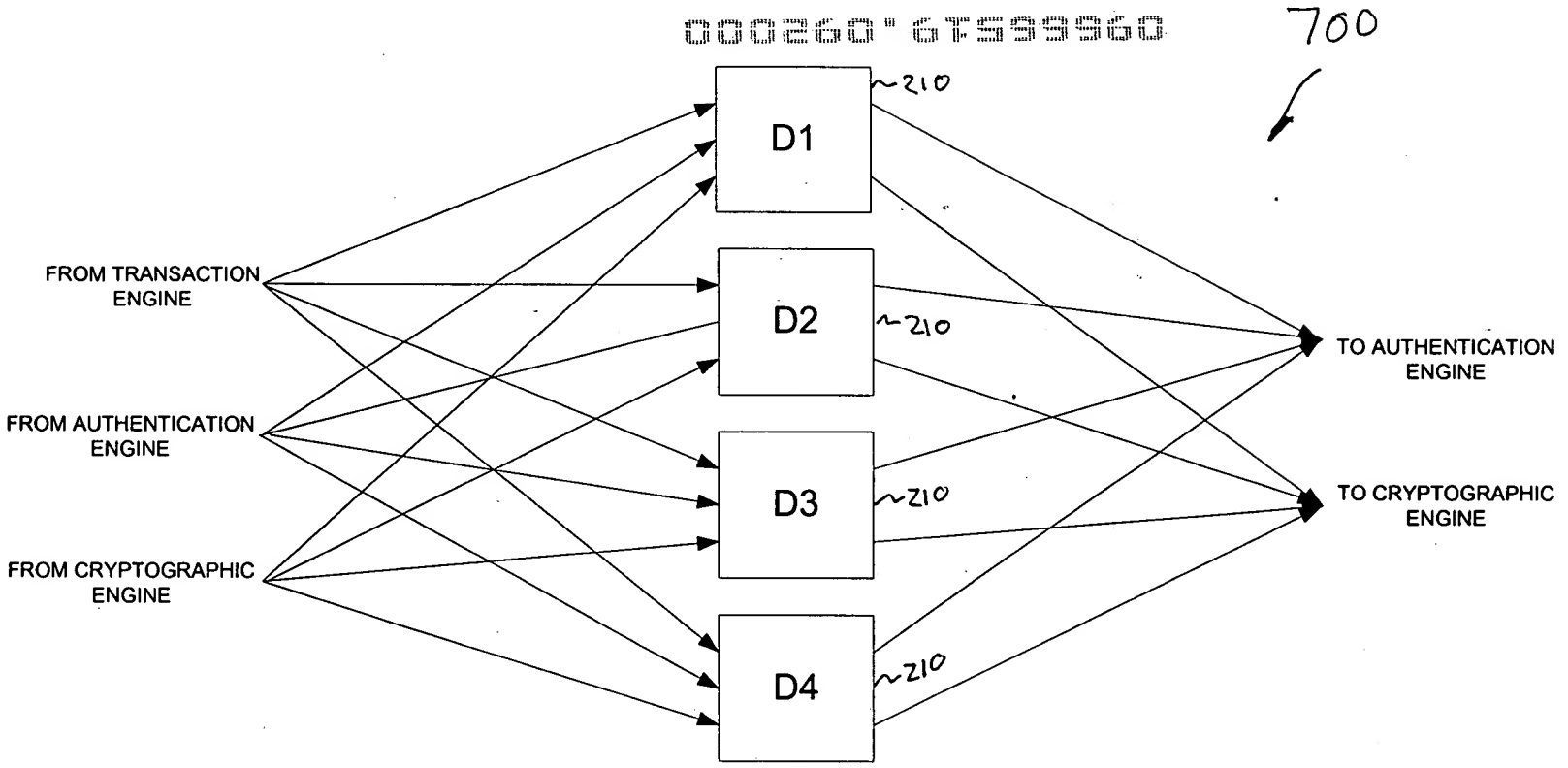


FIG. 7

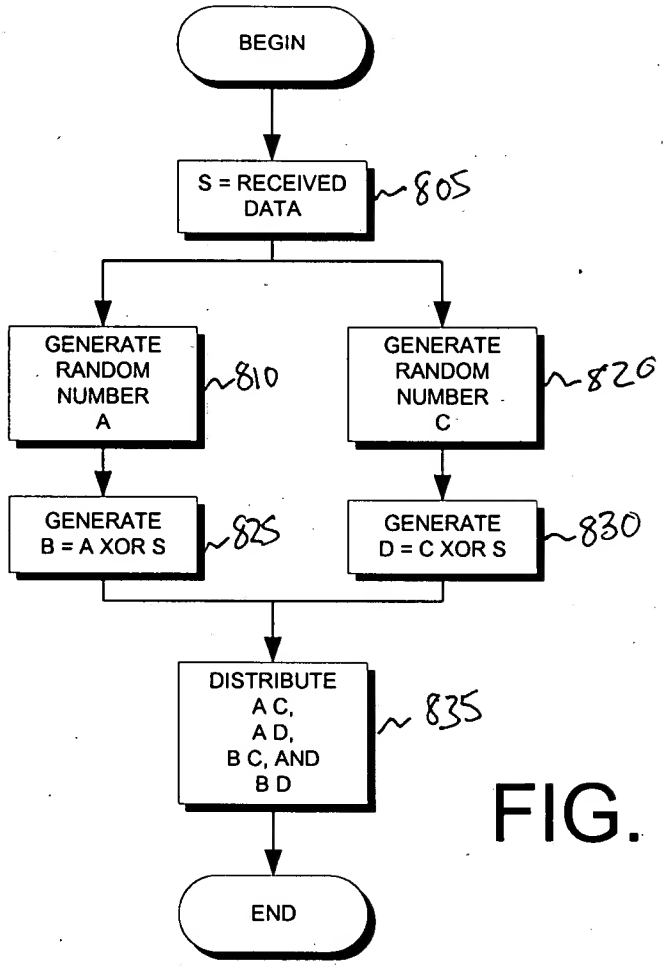

BEGIN
S = RECEIVED DATA
805
GENERATE RANDOM NUMBER A
810
GENERATE RANDOM NUMBER C
820
GENERATE B = A XOR S
825
GENERATE D = C XOR S
830
DISTRIBUTE A C, A D, B C, AND B D
835
END
800

FIG. 8

900

ENROLLMENT DATA FLOW			
SEND	**RECEIVE**	**SSL**	**ACTION**
USER	TRANSACTION ENGINE (TE)	½	TRANSMIT ENROLLMENT AUTHENTICATION DATA (B) AND THE USER ID (UID) ENCRYPTED WITH THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(UID, B))
TE	AE	FULL	FORWARD TRANSMISSION
			AE DECRYPTS AND SPLITS FORWARDED DATA
AE	THE X^{TH} DEPOSITORY (DX)	FULL	STORE RESPECTIVE PORTION OF DATA
WHEN DIGITAL CERTIFICATE REQUESTED			
AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST KEY GENERATION
			CE GENERATES AND SPLITS KEY
CE	TE	FULL	TRANSMIT REQUEST FOR DIGITAL CERTIFICATE
TE	CERTIFICATION AUTHORITY (CA)	½	TRANSMIT REQUEST
CA	TE	½	TRANSMIT DIGITAL CERTIFICATE
TE	USER	½	TRANSMIT DIGITAL CERTIFICATE
TE	MS	FULL	STORE DIGITAL CERTIFICATE
CE	DX	FULL	STORE RESPECTIVE PORTION OF KEY

FIG. 9A

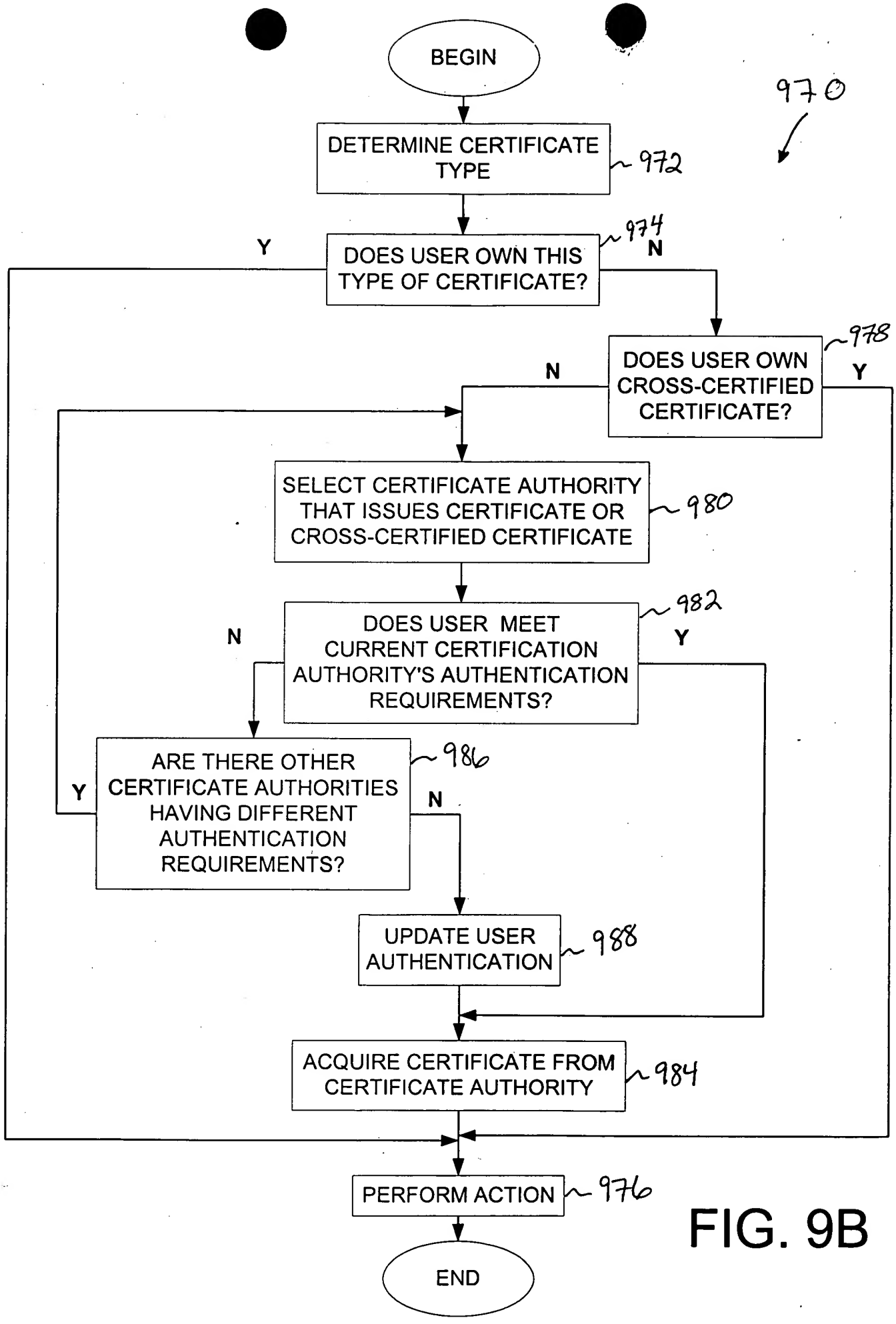

BEGIN
970
DETERMINE CERTIFICATE TYPE
972
DOES USER OWN THIS TYPE OF CERTIFICATE?
974
Y
N
DOES USER OWN CROSS-CERTIFIED CERTIFICATE?
978
N
Y
SELECT CERTIFICATE AUTHORITY THAT ISSUES CERTIFICATE OR CROSS-CERTIFIED CERTIFICATE
980
DOES USER MEET CURRENT CERTIFICATION AUTHORITY'S AUTHENTICATION REQUIREMENTS?
982
N
Y
ARE THERE OTHER CERTIFICATE AUTHORITIES HAVING DIFFERENT AUTHENTICATION REQUIREMENTS?
986
Y
N
UPDATE USER AUTHENTICATION
988
ACQUIRE CERTIFICATE FROM CERTIFICATE AUTHORITY
984
PERFORM ACTION
976
END

FIG. 9B

1000

	AUTHENTICATION DATA FLOW			
	SEND	**RECEIVE**	**SSL**	**ACTION**
1005	USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS SELECTING PURCHASE
1010	VENDOR	USER	½	TRANSMIT TRANSACTION ID (TID), AND AUTHENTICATION REQUEST (AR)
				AUTHENTICATION DATA (B') IS GATHERED FROM USER
1015	USER	TE	½	TRANSMIT TID AND B' WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE), AS (PUB_AE(TID, B'))
1020	TE	AE	FULL	FORWARD TRANSMISSION
				ENROLLMENT AUTHENTICATION DATA (B) IS REQUESTED AND GATHERED
1025	VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS TID, AR
1030	TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
1035	TE	THE X^{TH} DEPOSITORY (DX)	FULL	UID, TID
1040	DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
1045				AE ASSEMBLES B AND COMPARES TO B'
1050	AE	TE	FULL	TID, THE FILLED IN AR
1055	TE	VENDOR	FULL	TID, YES/NO
	TE	USER	½	TID, CONFIRMATION MESSAGE

FIG. 10

1100

SIGNING DATA FLOW			
SEND	**RECEIVE**	**SSL**	**ACTION**
USER	VENDOR	½	TRANSACTION OCCURS, SUCH AS AGREEING ON A DEAL
VENDOR	USER	½	TRANSMIT TRANSACTION IDENTIFICATION NUMBER (TID), AUTHENTICATION REQUEST (AR), AND AGREEMENT OR MESSAGE (M)
			CURRENT AUTHENTICATION DATA (B') AND A HASH OF THE MESSAGE RECEIVED BY THE USER (h(M')) IS GATHERED FROM USER
USER	TE	½	TRANSMIT TID, B', AR, AND h(M') WRAPPED IN THE PUBLIC KEY OF THE AUTHENTICATION ENGINE (AE) AS (PUB_AE(TID, B', h(M'))
TE	AE	FULL	FORWARD TRANSMISSION
			GATHER ENROLLMENT AUTHENTICATION DATA
VENDOR	TRANSACTION ENGINE (TE)	FULL	TRANSMITS UID, TID, AR, AND A HASH OF THE MESSAGE (h(M)).
TE	MASS STORAGE (MS)	FULL	CREATE RECORD IN DATABASE
TE	THE X^{TH} DEPOSITORY (DX)	FULL	UID, TID
DX	AE	FULL	TRANSMIT THE TID AND THE PORTION OF THE AUTHENTICATION DATA STORED AT ENROLLMENT (BX) AS (PUB_AE(TID, BX))
			THE ORIGINAL VENDOR MESSAGE IS TRANSMITTED TO THE AE
TE	AE	FULL	TRANSMIT h(M)
			AE ASSEMBLES B, COMPARES TO B' AND COMPARES h(M) TO h(M')
AE	CRYPTOGRAPHIC ENGINE (CE)	FULL	REQUEST FOR DIGITAL SIGNATURE AND A MESSAGE TO BE SIGNED, FOR EXAMPLE, THE HASHED MESSAGE
AE	DX	FULL	TID, SIGNING UID
DX	CE	FULL	TRANSMIT THE PORTION OF THE CRYPTOGRAPHIC KEY CORRESPONDING TO THE SIGNING PARTY
			CE ASSEMBLES KEY AND SIGNS
CE	AE	FULL	TRANSMIT THE DIGITAL SIGNATURE (S) OF SIGNING PARTY
AE	TE	FULL	TID, THE FILLED IN AR, h(M), AND S
TE	VENDOR	FULL	TID, A RECEIPT = (TID, YES/NO, AND S), AND THE DIGITAL SIGNATURE OF THE TRUSTENGINE, FOR EXAMPLE, A HASH OF THE RECEIPT ENCRYPTED WITH THE TRUSTENGINE'S PRIVATE KEY (Priv_TE(h(RECEIPT)
TE	USER	½	TID, CONFIRMATION MESSAGE

103 105 1110 1115 1120 1125 1130 1135 1140

FIG. 11

1200

ENCRYPTION/DECRYPTION DATA FLOW			
SEND	**RECEIVE**	**SSL**	**ACTION**
DECRYPTION			
			PERFORM AUTHENTICATION DATA PROCESS 1000, INCLUDE THE SESSION KEY (SYNC) IN THE AR, WHERE THE SYNC HAS BEEN ENCRYPTED WITH THE PUBLIC KEY OF THE USER AS PUB_USER(SNYC)
			AUTHENTICATE THE USER
AE	CE	FULL	FORWARD PUB_USER(SYNC) TO CE
AE	DX	FULL	UID, TID
DX	CE	FULL	TRANSMIT THE TID AND THE PORTION OF THE PRIVATE KEY AS (PUB_AE(TID, KEY_USER))
			CE ASSEMBLES THE CRYPTOGRAPHIC KEY AND DECRYPTS THE SYNC
CE	AE	FULL	TID, THE FILLED IN AR INCLUDING DECRYPTED SYNC
AE	TE	FULL	FORWARD TO TE
TE	REQUESTING APP/VENDOR	½	TID, YES/NO, SYNC
ENCRYPTION			
REQUESTING APP/VENDOR	TE	½	REQUEST FOR PUBLIC KEY OF USER
TE	MS	FULL	REQUEST DIGITAL CERTIFICATE
MS	TE	FULL	TRANSMIT DIGITAL CERTIFICATE
TE	REQUESTING APP/VENDOR	½	TRANSMIT DIGITAL CERTIFICATE

1205 1210 1215 1220 1225 1230 1235 1240 1245 1250

FIG. 12

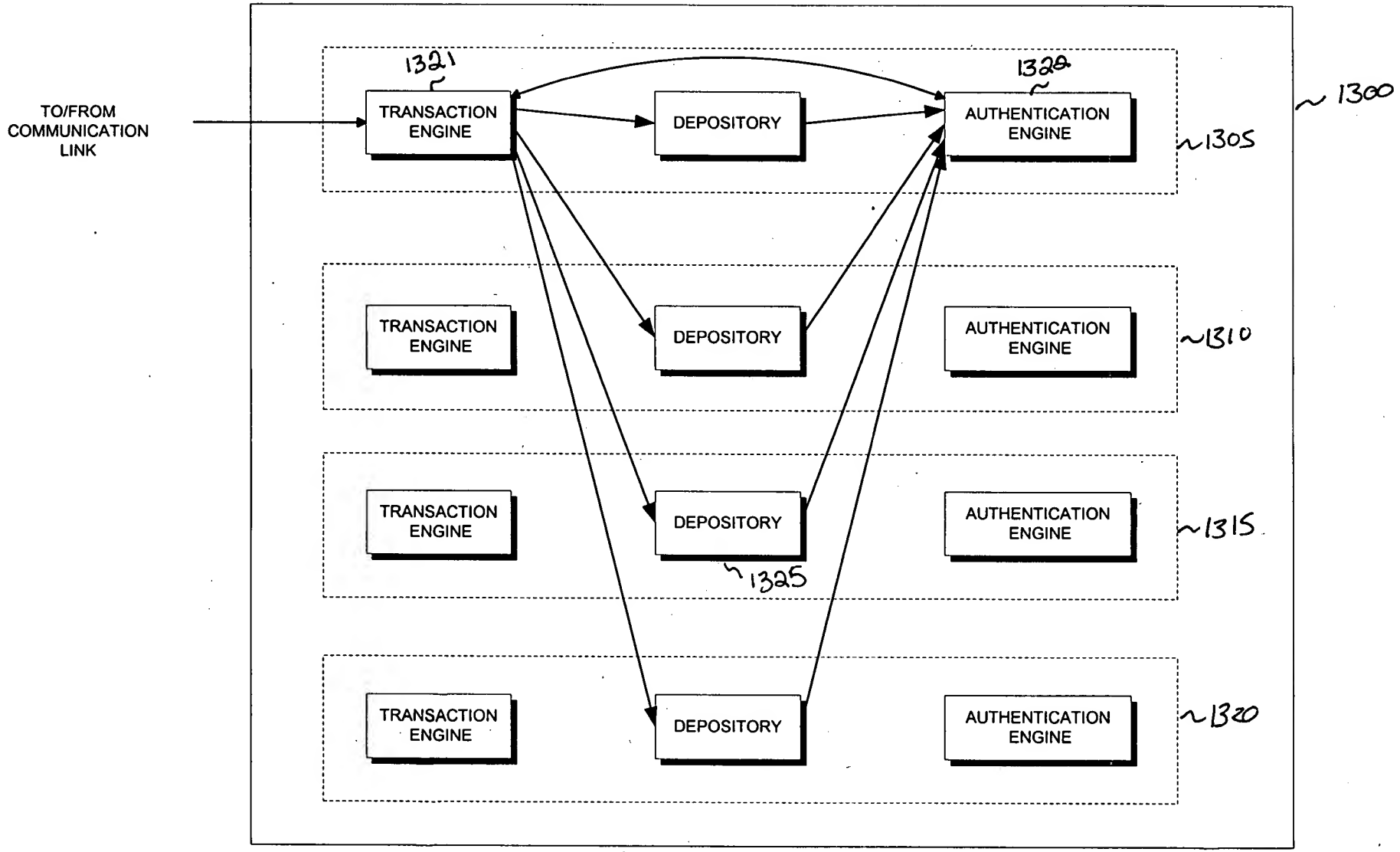


FIG. 13

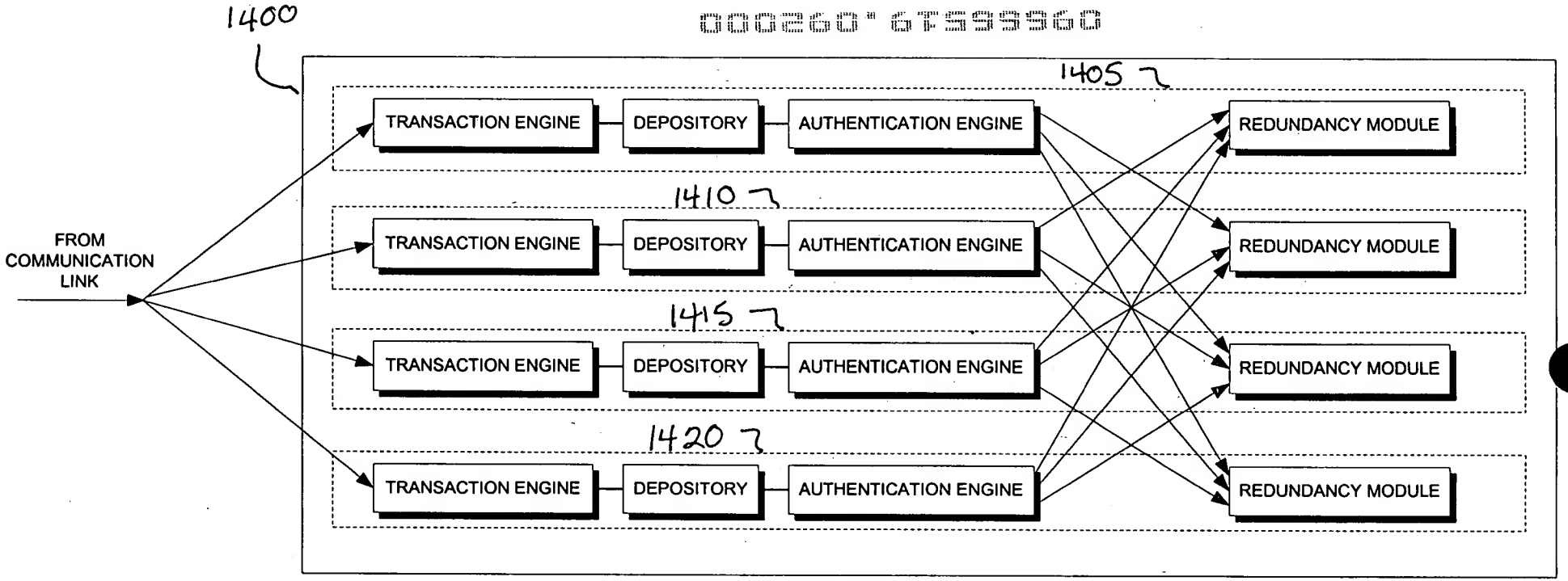

1400
1405
1410
1415
1420
FROM COMMUNICATION LINK
TRANSACTION ENGINE
DEPOSITORY
AUTHENTICATION ENGINE
REDUNDANCY MODULE

FIG. 14

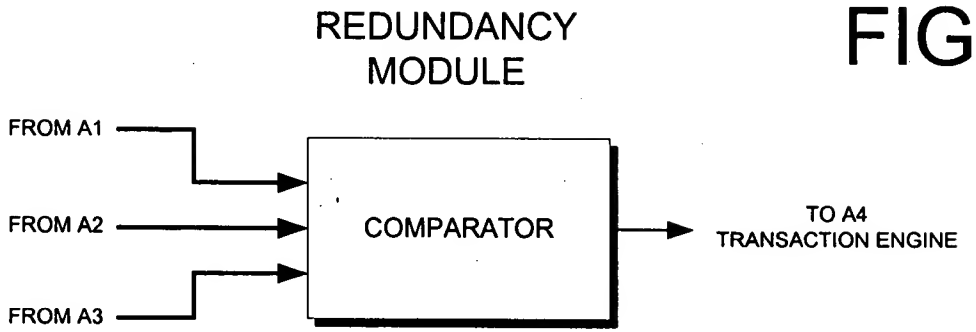

REDUNDANCY MODULE
FROM A1
FROM A2
FROM A3
COMPARATOR
TO A4 TRANSACTION ENGINE

FIG. 15

FIGURE 16

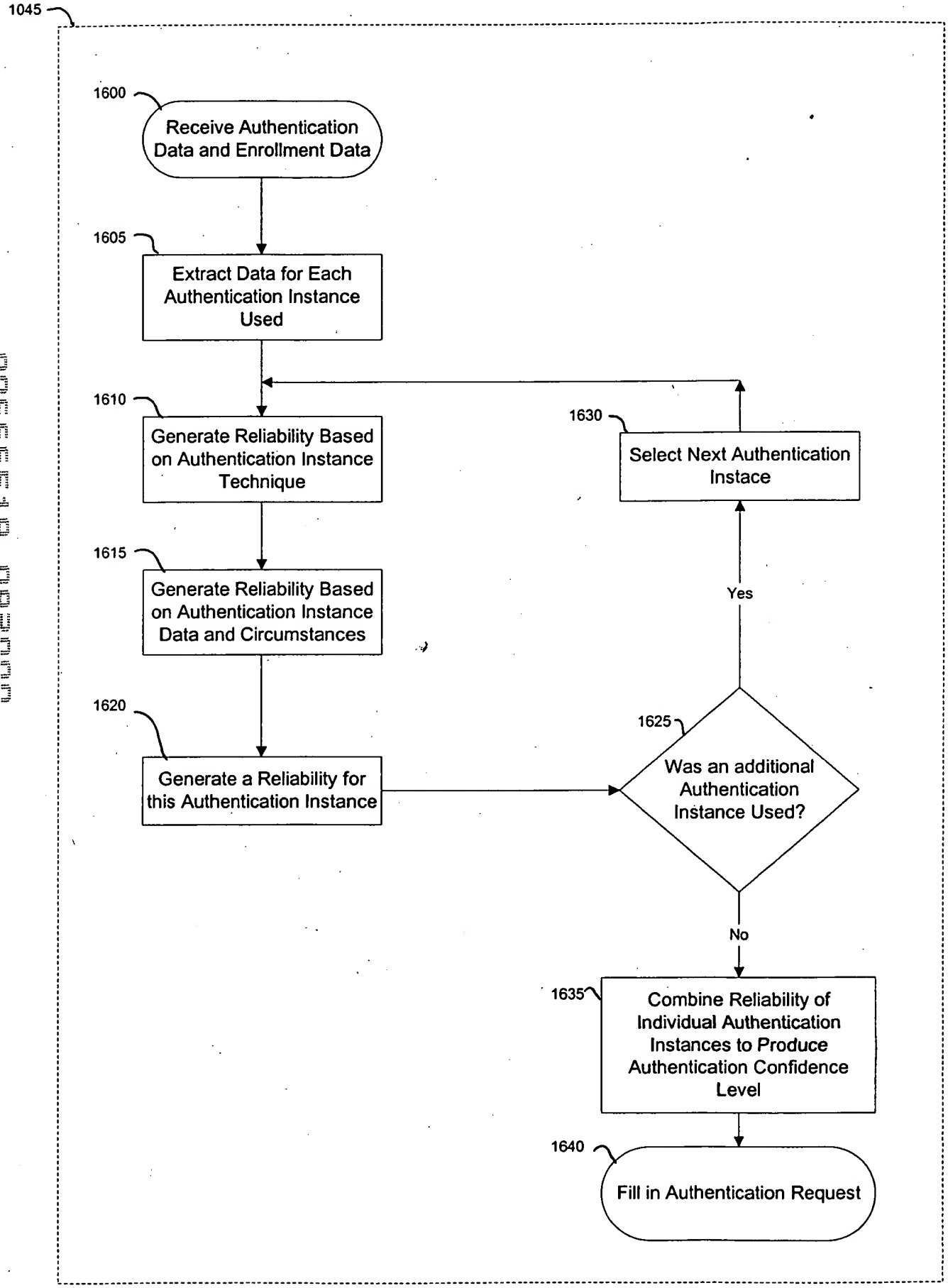

1045
1600
Receive Authentication Data and Enrollment Data
1605
Extract Data for Each Authentication Instance Used
1610
Generate Reliability Based on Authentication Instance Technique
1615
Generate Reliability Based on Authentication Instance Data and Circumstances
1620
Generate a Reliability for this Authentication Instance
1625
Was an additional Authentication Instance Used?
Yes
1630
Select Next Authentication Instace
No
1635
Combine Reliability of Individual Authentication Instances to Produce Authentication Confidence Level
1640
Fill in Authentication Request

FIGURE 17

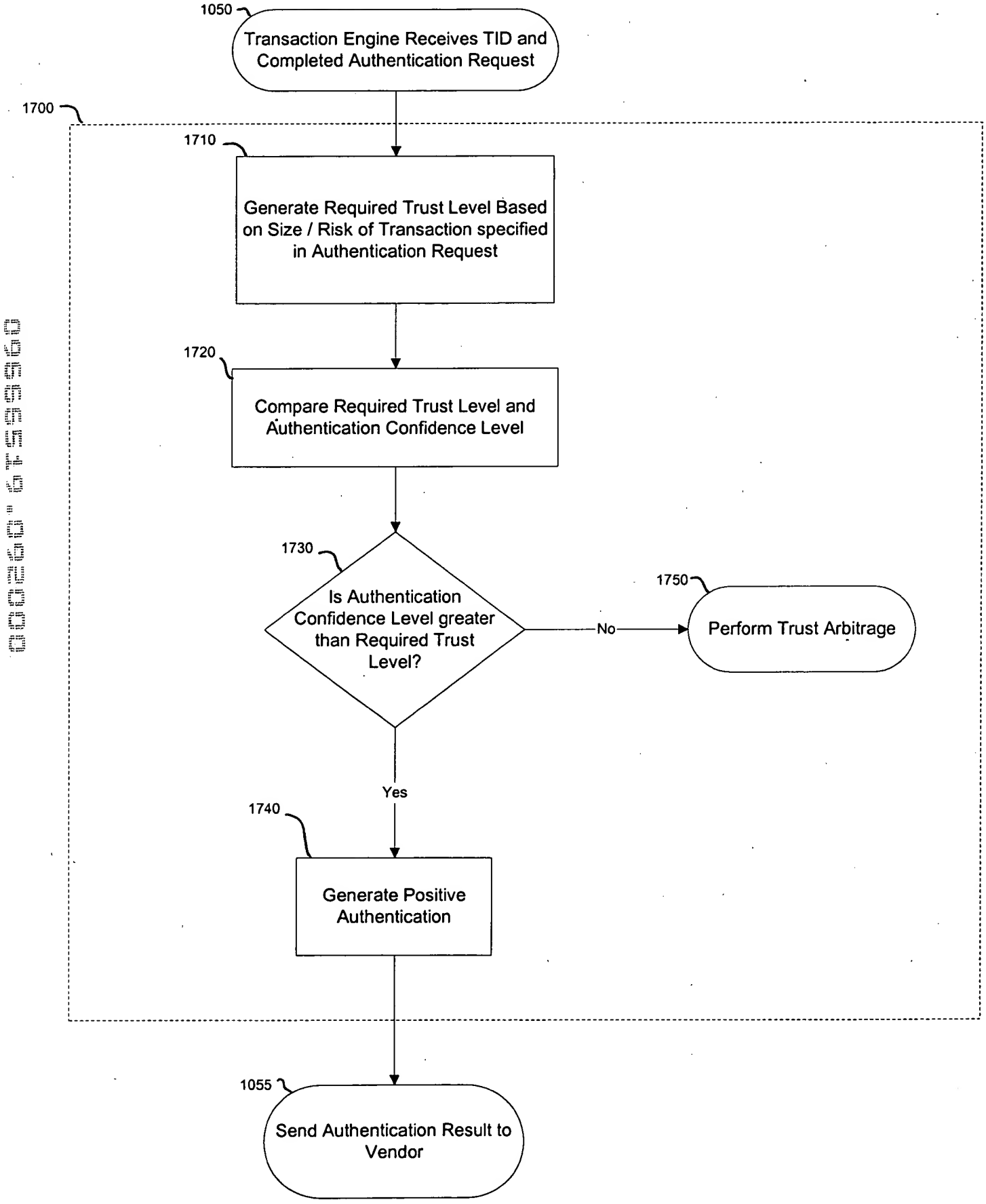

1050
Transaction Engine Receives TID and Completed Authentication Request
1700
1710
Generate Required Trust Level Based on Size / Risk of Transaction specified in Authentication Request
1720
Compare Required Trust Level and Authentication Confidence Level
1730
Is Authentication Confidence Level greater than Required Trust Level?
No
1750
Perform Trust Arbitrage
Yes
1740
Generate Positive Authentication
1055
Send Authentication Result to Vendor

FIGURE 18

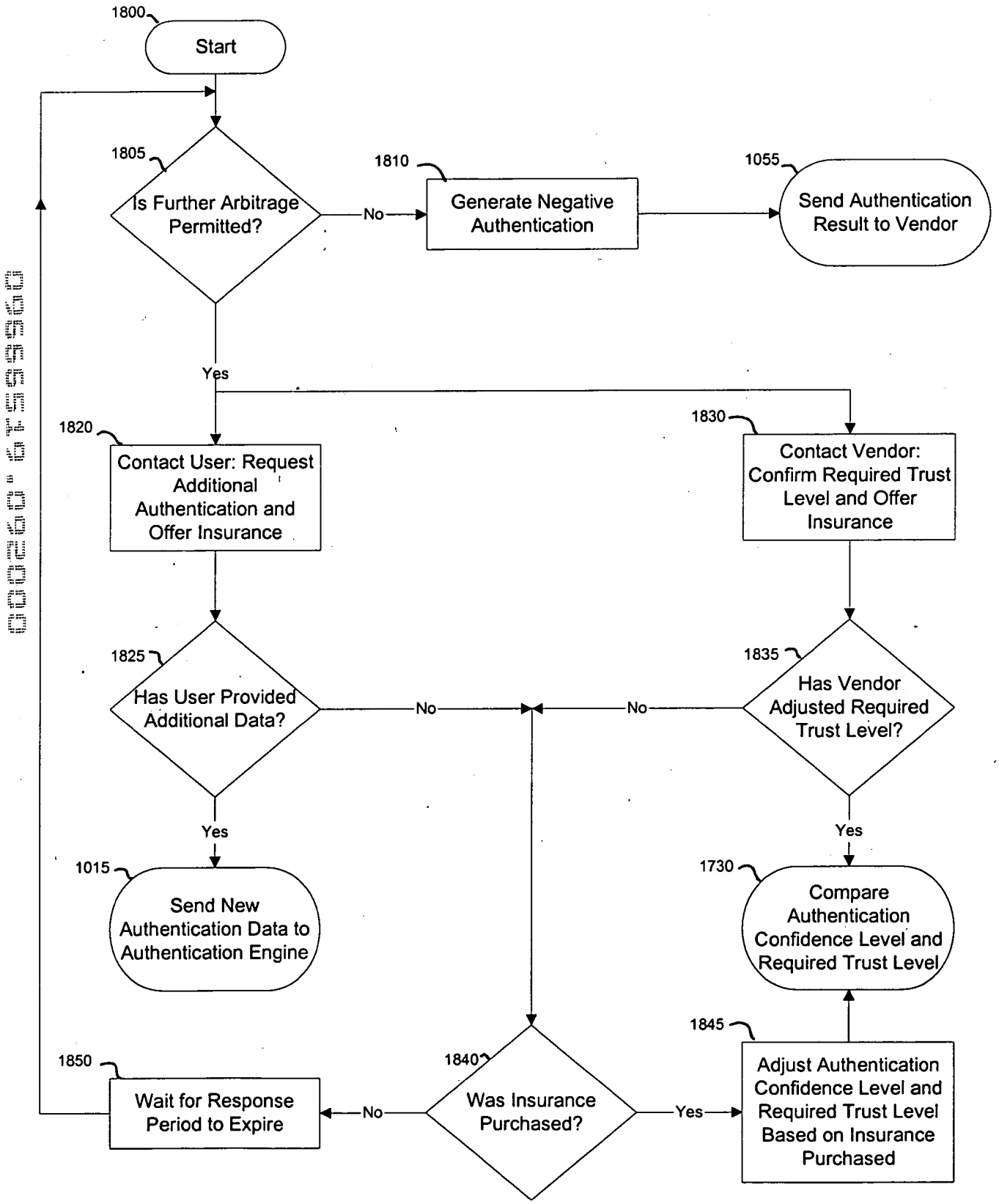

1800
Start
1805
Is Further Arbitrage Permitted?
No
1810
Generate Negative Authentication
1055
Send Authentication Result to Vendor
Yes
1820
Contact User: Request Additional Authentication and Offer Insurance
1830
Contact Vendor: Confirm Required Trust Level and Offer Insurance
1825
Has User Provided Additional Data?
No
No
1835
Has Vendor Adjusted Required Trust Level?
Yes
Yes
1015
Send New Authentication Data to Authentication Engine
1730
Compare Authentication Confidence Level and Required Trust Level
1845
Adjust Authentication Confidence Level and Required Trust Level Based on Insurance Purchased
1840
Was Insurance Purchased?
No
Yes
1850
Wait for Response Period to Expire

FIGURE 19

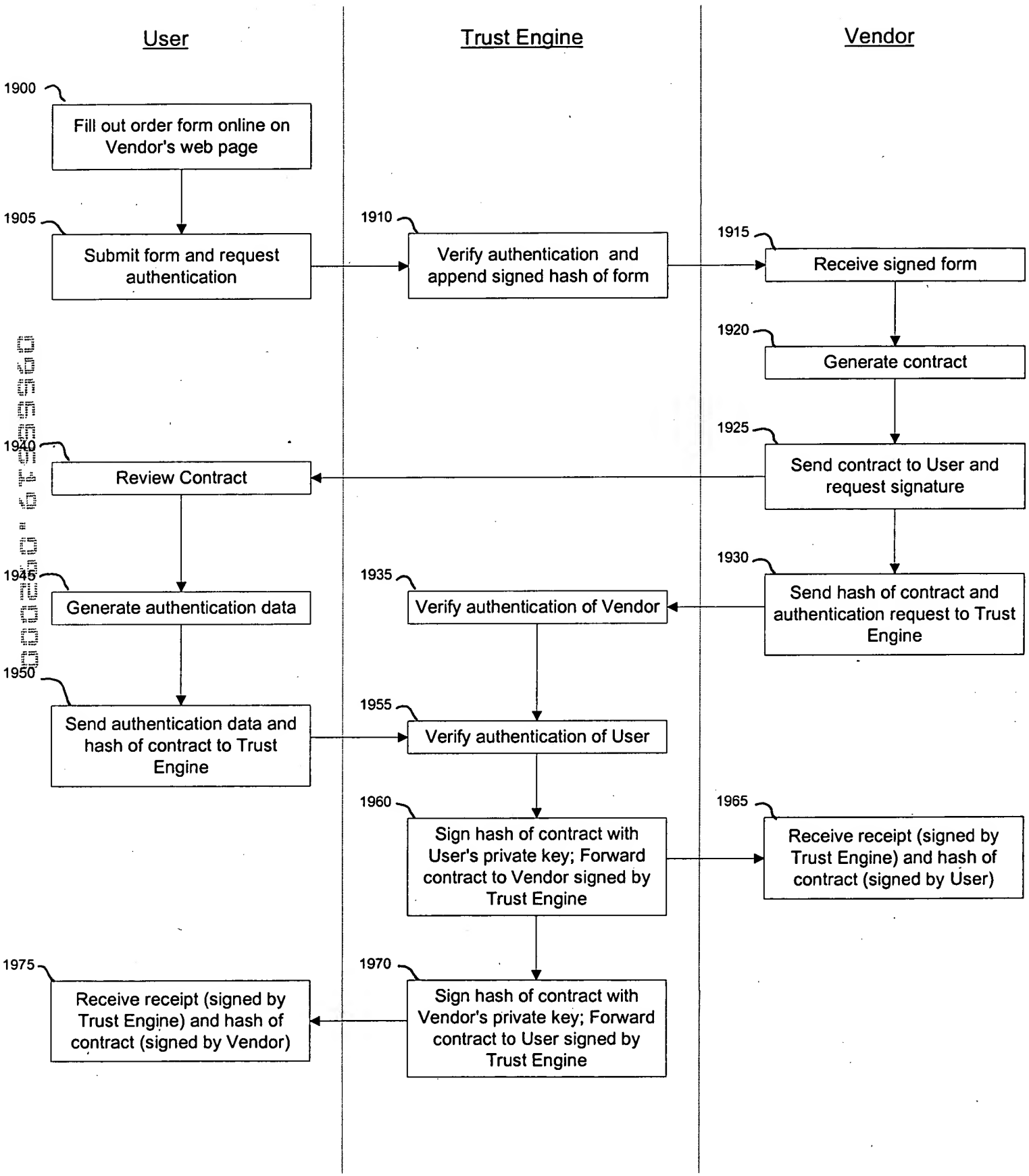
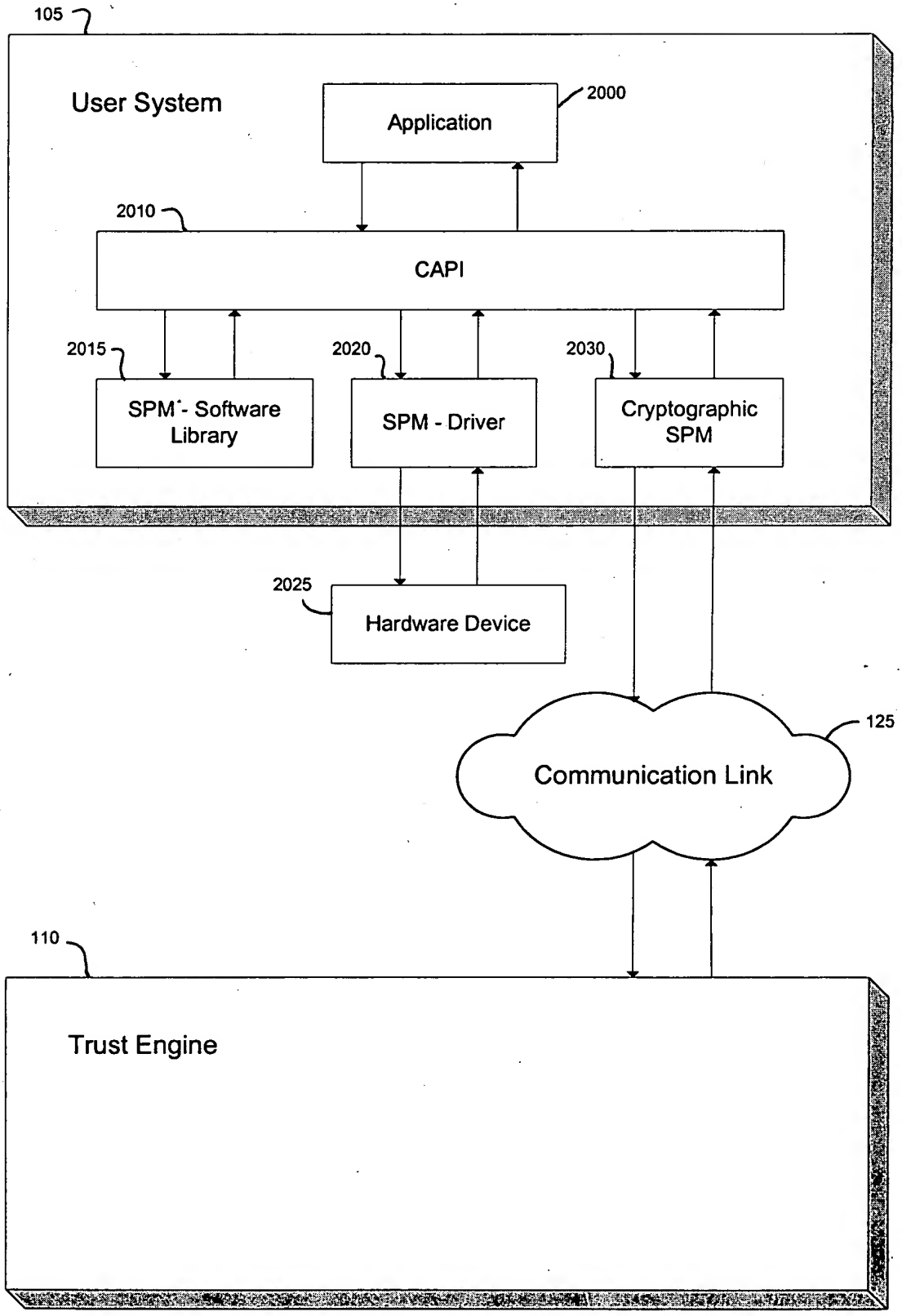

User
Trust Engine
Vendor
1900
Fill out order form online on Vendor's web page
1905
Submit form and request authentication
1910
Verify authentication and append signed hash of form
1915
Receive signed form
1920
Generate contract
1925
Send contract to User and request signature
1930
Send hash of contract and authentication request to Trust Engine
1935
Verify authentication of Vendor
1940
Review Contract
1945
Generate authentication data
1950
Send authentication data and hash of contract to Trust Engine
1955
Verify authentication of User
1960
Sign hash of contract with User's private key; Forward contract to Vendor signed by Trust Engine
1965
Receive receipt (signed by Trust Engine) and hash of contract (signed by User)
1970
Sign hash of contract with Vendor's private key; Forward contract to User signed by Trust Engine
1975
Receive receipt (signed by Trust Engine) and hash of contract (signed by Vendor)

FIGURE 20


105
User System
Application
2000
2010
CAPI
2015
SPM - Software Library
2020
SPM - Driver
2030
Cryptographic SPM
2025
Hardware Device
125
Communication Link
110
Trust Engine